AMENDMENT TO THE CLAIMS

1. (Currently Amended) A computer-implemented method for providing data security, the method comprising:

receiving a password from a user, the password being the user's password;

utilizing the password to encrypt an encryption component, wherein utilizing the password comprises applying the password to the encryption component so as to produce a ~~as a basis for generation of a~~ user-specifically encrypted version of ~~an~~ the encryption component, the user-specifically encrypted version being user-specific in that the encryption process applied to the encryption component factors in the user's password, and wherein the encryption component ~~being~~ is a collection of data that specifies an encryption or decryption process;

storing the user-specifically encrypted version of the encryption component, wherein storing comprises storing the user-specifically encrypted version of the encryption component within a record that is associated with the user;

selectively allowing the user to process the user-specifically encrypted version of the encryption component so as to derive the encryption component, wherein selectively allowing further comprises selectively allowing the user to decrypt the user-specifically encrypted version of the encryption component so as to regain access to the encryption component itself; ~~and~~

utilizing the decrypted encryption component to process sensitive data; ~~.~~

receiving a second password from a different user, the second password being the different user's password; and

utilizing the second password to encrypt the encryption

component, wherein utilizing the second password comprises applying the second password to the encryption component so as to produce a second user-specifically encrypted version of the encryption component, the second user-specifically encrypted version being user-specific in that the encryption process applied to the encryption component factors in the different user's password; and

storing the second user-specifically encrypted version of the encryption component, wherein storing comprises storing the second user-specifically encrypted version of the encryption component within a record that is associated with the different user.

2. (Cancelled)

3. (Cancelled)

4. (Original) The method of claim 1, further comprising:
generating an encrypted version of the password; and
storing the encrypted version of the password.

5. (Original) The method of claim 4, wherein storing the encrypted version of the password comprises storing the encrypted version of the password within a record that is associated with the user.

6. (Original) The method of claim 4, wherein generating an encrypted version of the password comprises encrypting the password based on a one-way hash function.

7. (Cancelled)

8. (Cancelled)

9. (Currently Amended) The method of claim 1~~7~~, further

comprising:

generating an encrypted version of the second password; and

storing the encrypted version of the second password within a record that is associated with the second user.

10. (Original) The method of claim 1, further comprising:

receiving an administrator password from an administrator; and

utilizing the administrator password as a basis for generation of an administrator-specific version of the encryption component; and

storing the administrator-specific version of the encryption component.

11. (Original) The method of claim 10, wherein storing comprises storing the administrator-specific version of the encryption key within a record that is associated with the administrator.

12. (Original) The method of claim 10, further comprising:

generating an encrypted version of the administrator password; and

storing the encrypted version of the administrator password within a record that is associated with the administrator.

13. (Currently Amended) The method of claim 1, wherein ~~utilizing the password as a basis for generation of a user-specific version of an~~ the encryption component ~~comprises utilizing the password as a basis for generation of~~is ~~a user-specific version of~~ an application security key.

14. (Currently Amended) A computer-readable medium having instructions embedded thereon that, when executed, cause a computer to carry out a method comprising the steps of:

obtaining an encryption component; and

creating and storing a plurality of user-specific versions of

the encryption component;

selectively allowing users to process their version of the encryption component so as to derive the encryption component, wherein selectively allowing further comprises selectively allowing a given user to decrypt their version of the encryption component so as to undo what made their version user-specific, thereby enabling access to the encryption component itself, and wherein selectively allowing still further comprises authenticating users and only allowing authorized users to process their version of the encryption component to derive the encryption component; and

utilizing the encryption component to process sensitive data.

15. (Original) The method of claim 14, wherein storing a plurality of user-specific versions comprises storing a user-specific version in a user account for each of a plurality of users.

16. (Original) The method of claim 14, wherein obtaining an encryption component comprises obtaining an application security encryption key.

17. (Original) The method of claim 14, wherein creating a plurality of user-specific versions comprises encrypting the encryption component based on a plurality of different user passwords.

18. (Cancelled)

19. (Currently Amended) The method of claim ~~18~~14, wherein authenticating users comprises, for each user:

receiving a password;

processing the password to generate an encrypted version; and

comparing the encrypted version to an authorized value.

20. (Original) The method of claim 19, wherein processing the password comprising applying a one-way hash algorithm.

21. (Currently Amended) A computer implemented method of providing data security, the method comprising:

receiving a password from a user;

processing the password to form an encrypted version;

comparing the encrypted version to a list of authorized values stored in a database;

if the encrypted version matches an authorized value, and if doing so would be consistent with a plurality of allocated user access privileges, utilizing the password as a basis for decrypting a user-specific version of an encryption component, the encryption component being a collection of data that specifies an encryption or decryption process; ~~and~~

utilizing the encryption component to process sensitive data; and

wherein the plurality of allocated user access privileges are distributed based on a plurality of user roles, and wherein the method further comprises making the step of utilizing the encryption component contingent upon the user being associated with a particular user role.

22. (Cancelled)

23. (Original) The method of claim 21, wherein the plurality of allocated user access privileges are distributed based on user identity, and wherein the method further comprises making the steps of utilizing the encryption component contingent upon the user having a particular identity.